Identity Theft Prevention, Identification and Mitigation

Are you as safe as you think you are?

Identity Theft

9.3M - 8.9 Million Adult Americans in 2005
Total Losses $5.44 – $5.66 Billion
Average Losses $5,885 - $6,383
Median fraud amount per fraud victim $750 - $750
Average consumer cost $675 - $422
Average resolution time 28 hours - 40 hours
Median resolution time 5 hours - 5 hours
68.2% Paper-based Theft
11.6% Computer Crime
50% Family Members, Friends, and Neighbors
28.8% Lost or Stolen Wallets and Checkbooks

Introduction

The 1990's spawned a new variety of crooks called identity thieves.

•Their target = your everyday financial transactions.

•Their intent is to commit fraud or theft.

•Months or years — and thousands of dollars — spent each year cleaning up the mess the thieves have made of good names and credit records.

•Identity theft results in lose of job opportunities, loans for education, housing, cars, or even arrests for crimes people didn't commit.

Introduction

Identity theft – What is it?

The manipulation of, or improperly accessing, another person's identifying information, such as social security number, mother's maiden name, or personal identification number (rather than account number) in order to fraudulently establish credit or take over a deposit, credit or other financial account for benefit.

It's The Law

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) is the federal law making identity theft a crime.

The Act makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under the Act, a name or SSN is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Violations of the Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and SSA's office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

How Identity Theft Occurs

Despite best efforts, skilled identity thieves gain access to your data.

•They steal wallets and purses.

•They steal your mail or divert your mail to another location.

•They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”

•They fraudulently obtain your credit report.

How Identity Theft Occurs

Despite best efforts, skilled identity thieves gain access to your data.

•They find personal information in your home.

•They use personal information you share on the Internet (11.6%).

•They get your information from the businesses in a practice known as "business record theft" (customer, employee, patient or student; bribing an employee who has access to your files; or "hacking" into electronic files).

They get your information from the businesses…
"hacking" into electronic files.

DAILY BRIEFING
May 1, 2006

Hackers access personal information on TRICARE servers

By Daniel Pulliam
dpulliam@govexec.com

Hackers gained access to the Pentagon's health insurance information systems, compromising the personal information of more than 14,000 people…

The intrusion of the TRICARE Management Activity public computer servers was discovered on April 5...The hacked information included databases of names, Social Security numbers, the last four digits of credit card numbers, personal phone numbers, work and personal e-mail addresses and home addresses.

The Defense Criminal Investigative Service is participating in an investigation of the incident.

The department sent affected people letters informing them that the compromise of their personal information could put them at risk for identity theft and recommending precautionary measures.

"A security problem of this magnitude on this level underscores the need to address security as a fundamental issue on the development and implementation of any national electronic health care record initiative," McNulty said.

They scam you, often through email, by posing as legitimate companies or government agencies you do business with

Phishing

- Phishing attacks grew by 28 % from May 04 to May 05
- 73 Million adult email users reported more than 50 phishing emails during the 12 month period
- 11 million recipients of phishing emails clicked on the links, since May 03
- 1.8 million reported providing personal information
- 2.42 million adults reported losing money because of phishing attacks ($929 million)
- 150 to 200 uniquely identifiable phishing attacks against Major US Internet service providers reported
- Pay Pal and E bay are the top spoofed sites. Citibank is the primary bank target for phishing scams

More Phishing…

Dear Customer,
Our records show that Your VISA debit account has been inactive more than 3 months. In order to confirm your membership with us and avoid temporarily account suspension we will transfer a random amount between 0.25 USD and 0.99 USD into your debit card. This is a new security measure put in place by VISA to protect your account against unauthorized charges and account cancellation. To complete this process please, follow the link bellow:
Click Here

And more Phishing!

Dear VISA Credit Card Owner ,

VISA is devoted to keeping a safe environment for its community of consumers and producers. To guarantee the safety of your account, VISA deploys some of the most advanced security measures in the world and our anti-fraud units regularly screen the VISA database for suspicious activity.

We recently have discovered that multiple computers have attempted to log into your VISA. Online Banking account, and multiple password failures were presented before the logons. We now require you to re-validate your account information to us. If this is not completed by May 20, 2006, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

In order to confirm your Online Bank records, we may require some specific information from you. Please **Click Here** or on the link below to verify your account
http://www.visa.com/secure_update/update

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience. If you choose to ignore our request, you leave us no choice but to temporary suspend your account.

VISA Security Team

http:61.133.87.119;84/www.visa.com/visa.html

Expected Phishing!!

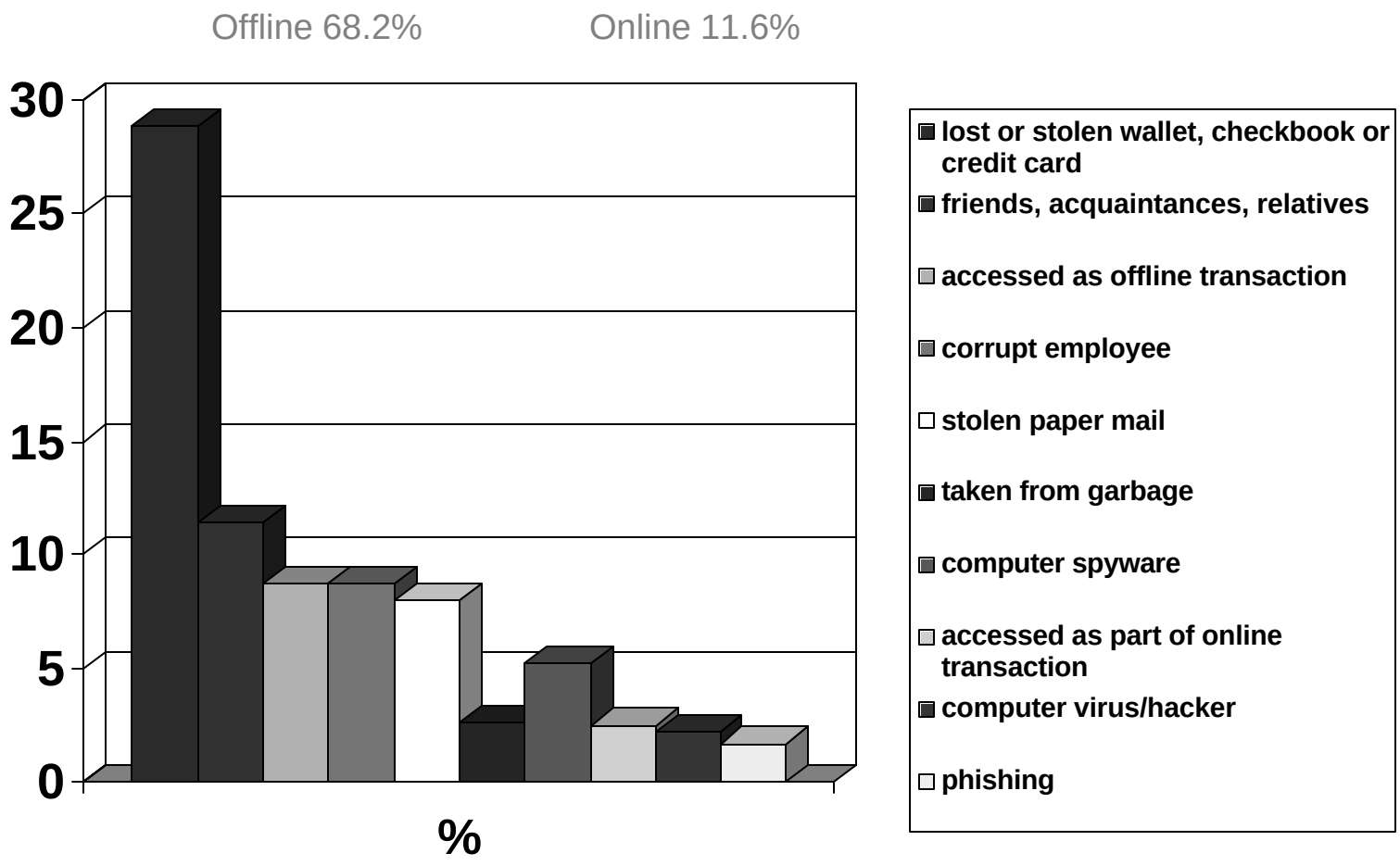
Dear Taxpayer

We have received your tax filing and are prepared to send your refund. However, we are experiencing difficulty in timely forwarding you refund to your bank and need your assistance.

Do not respond to this email for security purposes.

Go to our secure website at https:www.irs.gov/payments to complete the information required so we can forward your tax refund.

Offline Versus Online Methods of Access Causes Of Known Theft



Faster Detection = Lower Consumer Costs

47% of cases are detected by the victims first.

35% shorter detection times and 36% ($347) lower consumer costs reviewing credit reports or using a credit monitoring service ($264)

17% of cases are not detected at all until a creditor contacts the victim or until the victim applies for credit and is denied.

241 days to be discovered – cost consumer $1,391.

How Identity Theft Occurs

With Your Personal Information, Identity Thieves:

- Counterfeit checks or credit/debit cards on open accounts.
- Change the mailing address on your accounts.
- Open a new credit card, checking or wireless account.
- File for bankruptcy under your name.
- They buy cars by taking out auto loans in your name.
- They use your identity during an arrest.

Minimize Your Risk

Risk cannot be eliminated – but it can be minimized.

•Place passwords on your credit card, bank and phone accounts.

•Use a Firewall and Virus Protection and Anti-Spyware Software.

•Secure personal information in your home.

•Ask about information security procedures in your workplace.

•Routinely order a copy of your credit report from each of the three major credit bureaus.

•Expect your bills.

Minimize Your Risk

Maintaining Vigilance

•Don’t give out personal information on the phone, mail or over the Internet.

•Guard your mail and trash from theft.

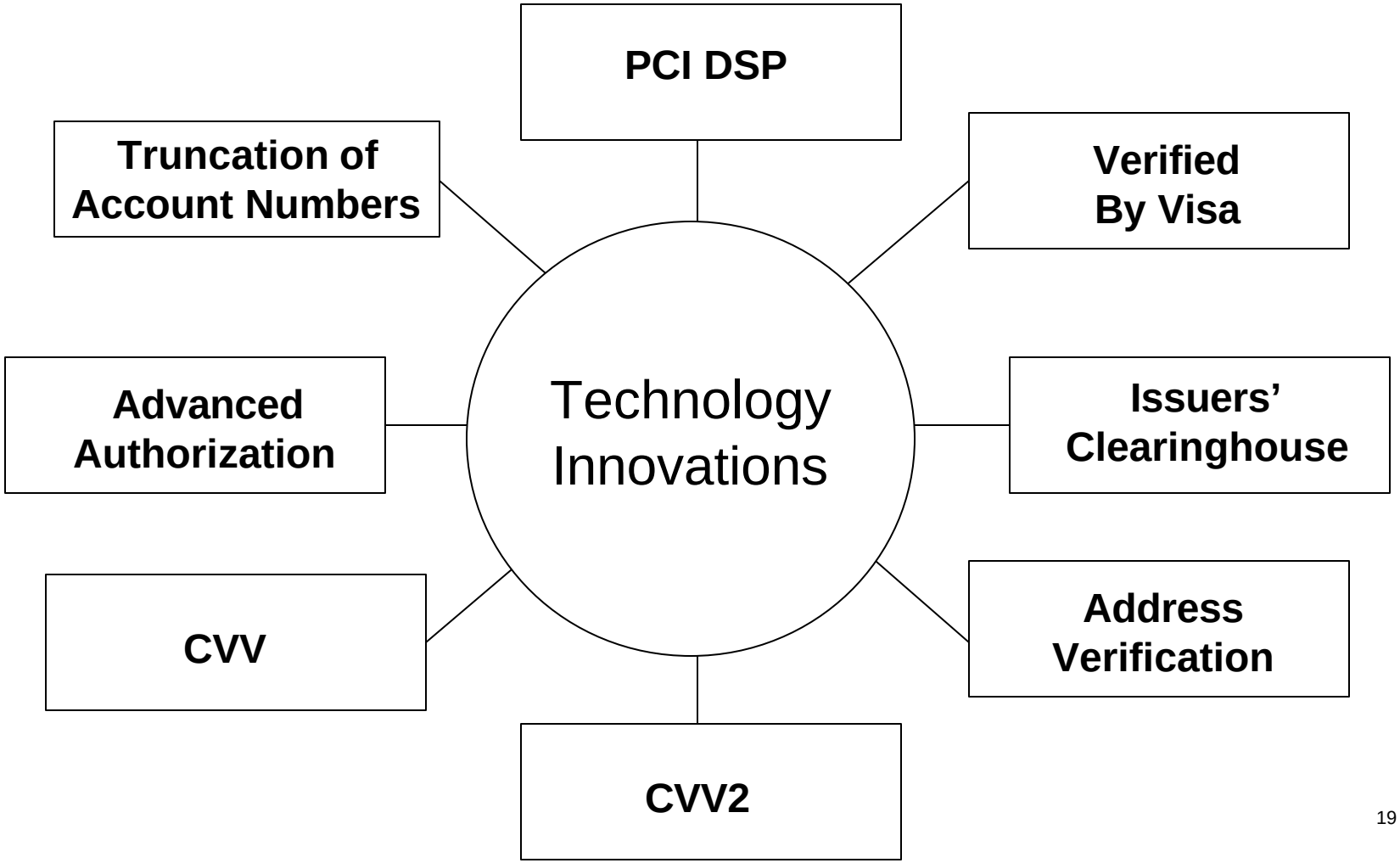
•Carry only the identification information and credit and debit cards that you’ll actually need.

•Give your SSN only when absolutely necessary.

•Be wary of promotional scams.

•Keep your purse or wallet in a safe place at work.

What's Visa doing?
Card Technological Safeguards



Payment Card Industry data Security Program (PCIDSP)

Who's minding the store?

Install firewalls
Never use vendors default passwords
Minimize storage of card data
Do not store track data
Encrypt data for backup/transmission
Make stored data unreadable
Regularly update antivirus software
Restrict data access to those whose jobs require it
Assign unique id to each user
Test systems regularly

If You're a Victim

Your First Five Steps

1. Notify Credit Bureaus and review your credit reports.

2. File a report with your local police or the police in the community where the identity theft took place.

3. Contact Fraud Department of Creditors.

4. File a complaint with the FTC.

5. Close any accounts that have been tampered with or opened fraudulently.

Are you Safe?
Take the Test!

www.idsafety.net

Are you a Victim?
Professional help available!

1-866-ID-HOTLINE, victims can receive free and confidential assistance from trained counselors.

References

CREDIT BUREAUS

For instant access to your free credit report (September 1, 2005 for Eastern US States) visit www.annualcreditreport.com

Request your Credit Report by Phone:
Call 1-877-322-8228

Request your Credit Report by Mail:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Consumer Opt-Out: 1-888-5-OPTOUT
www.optoutprescreen.com

References

CREDIT BUREAUS

Equifax — www.equifax.com

Experian — www.experian.com

TransUnion — www.transunion.com

Thank you for your attention!

Questions?